



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/882,491	06/15/2001	Yaron Goland	3382-53699	8148
26119	7590	05/16/2006	EXAMINER	
KLARQUIST SPARKMAN LLP			SON, LINH L D	
121 S.W. SALMON STREET			ART UNIT	
SUITE 1600			PAPER NUMBER	
PORTLAND, OR 97204			2135	

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/882,491

Applicant(s)

GOLAND, YARON

Examiner

Linh LD Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 February 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 02/27/06.
2. Claims 1-18 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al, US Patent No. 6772331B1, hereinafter "Hind", in view of Butt et al, US Patent No. 6754829B1, hereinafter "Butt".

5. As per claims 1-2, and 13:

Hind teaches "A branding process to establish cryptographically secured interaction among networked computing devices within a trust group on an open multi-access network, comprising:

securely networking a security-un-initialized device with a branding device via a secured network medium (Col 9 lines 25-40);

Art Unit: 2135

transmitting a branding certificate from the branding device to the security-un-initialized device via the secured network medium (Col 9 lines 25-40), the branding certificate instructing that the security-un-initialized device trust the branding device (Col 9 lines 15-60, creating a trust between the devices), the branding certificate further containing key data for verifying certificates provided by other devices on the open multi-access network to the security-un-initialized device are authenticated by the branding device (Col 9 lines 35-60);

transmitting a trust group membership certificate from the branding device to the security-un-initialized device via the secured network medium, the trust group membership certificate authenticating that the security-un-initialized device is a member of the trust group (Col 10 lines 18-29); and

initializing a security resolver of the security-un-initialized device to use the key data of the branding certificate to authenticate other devices interacting with the security-un-initialized device on the open multi-access network are in the trust group (Col 10 lines 18-29, and Col 11 line 5 to Col 12 line 20), and to provide the trust group membership certificate to such other devices as authentication that the security-un-initialized device is a member of the trust group (Col 10 lines 18-29, such that at least some interaction via the open multi-access network with the security-un-initialized device is cryptographically secured to only other devices in the trust group (Col 9 lines 15-60)).

However, Hind does not specifically disclose the certificate is a trust group membership certificate. Hind only disclose that the certificate is associated with the access control

Art Unit: 2135

groups and the certificate includes user group associations, access control groups fields.

Nevertheless, Butt discloses the "Certificate-Based Authentication System for Heterogeneous Environments", which includes issuing the certificate has group membership to access a certain resource (Col 3 line 45 to Col 4 line 12).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to realize that the Hind's certificate can also be authenticate to a group membership.

6. As per claim 3:

Hind and Butt teach "The branding process of claim 2 wherein securely networking the security-un-initialized and branding devices comprises networking the devices via a limited access network interface of the security-un-initialized device that is separate from the security-un-initialized device's interface to the open multi-access network" (Col 11 lines 5-65).

7. As per claim 4:

Hind and Butt teach "The branding process of claim 3 wherein the limited access network interface is of a direct device-to-device wired networking medium (Col 1 line 65 to Col 2 line 1).

8. As per claim 5:

Hind and Butt teach "The branding process of claim 3 wherein the limited access network interface is of a directional wireless networking medium" in (Col 1 line 55 to Col 2 line 10).

9. As per claim 6:

Hind and Butt teach "The branding process of claim 2 wherein securely networking the security-un-initialized and branding devices comprises: placing transmitter/receivers of the security-un-initialized and branding devices for an omni-directional wireless networking medium into a wave guide and/or Faraday cage; and networking the devices with the wave guide and/or Faraday cage via the omni-directional wireless networking medium" in (Col 1 line 55 to Col 2 line 10).

10. As per claim 7:

Hind and Butt teach "The branding process of claim 2 further comprising: transmitting a principal identifier from the branding device to the security-un-initialized device, the principal identifier providing a cryptographically secured identity to the security-un-initialized device, the principal identifier containing a public/private key pair; and using the public/private key pair to encrypt interaction of the security-un-initialized device with said other devices authenticated to be in the trust group" in (Col 11 lines 5-65).

11. As per claim 8:

Hind and Butt teach "The branding process of claim 7 wherein the principal identifier further contains a name for the security-un-initialized device, the process further comprising identifying the security-un-initialized device to human operators using the name" in (Col 12 lines 45-65).

12. As per claim 9:

Hind and Butt teach "The branding process of claim 8 further comprising prompting a human user of the branding device to enter the name upon performing the branding process on the security-un-initialized device" in (Col 12 lines 45-65).

13. As per claim 10:

Hind and Butt teach "The branding process of claim 2 further comprising initially distributing the security-un-initialized device in a retail channel prior to having the branding process performed on the security-un-initialized device" in (Col 5 lines 25).

14. As per claim 11:

Hind and Butt teach "The branding process of claim 10 further comprising upon completion of initializing the security resolver, disallowing the security-un-initialized device from having the branding process again performed on the security-un-initialized device until the now initialized security of the security-un-initialized device is reset" in

(Col 13lines 35-43).

15. As per claim 12:

Hind and Butt teach "The branding process of claim 10 further comprising upon completion of initializing the security resolver, allowing the branding process to be performed only via a limited access network interface of the security-un-initialized device" in (Col 4 line 53 to Col 5 line 5).

16. As per claim 14:

Hind and Butt teach "The networked computing device of claim 13 further comprising: a limited access networking interface; and the security initializer further operational to accept the branding public key when received from the branding device only via the limited access networking interface" in (Col 11 lines 5-45).

17. As per claim 15:

Hind and Butt teach "The networked computing device of claim 13 further comprising: the security initializer further operational to accept the branding public key when received from the branding device via the network interface when in an initial unbranded state; and a branding reset operational upon activation to return the security initializer to the initial unbranded state" in (Col 13 lines 35-43).

18. As per claim 16:

Hind and Butt teach "The networked computing device of claim 13 further comprising: a branding mode activator operational to place the networked computing device in a branding mode; and the security initializer further operational to accept the branding public key when received from the branding device via the network interface when in the branding mode" in (Col 11 lines 5-45).

19. As per claim 17:

Hind and Butt teach "The networked computing device of claim 13 further comprising: the security resolver further operational when initialized with a trust group membership certificate to provide the trust group membership certificate to other devices via the network interface to attest to membership of the networked computing in the trust group; and the security initializer further operational to receive the trust group membership certificate from the branding device while securely networked to the networked computing device, and further operational to initialize the security resolver with the trust group membership certificate" in (Col 9 lines 15-65, and Col 10 lines 24-30).

20. As per claim 18:

Hind and Butt teach "The networked computing device of claim 13 further comprising: the security resolver further operational when initialized with a public/private key pair to encrypt interaction via the network interface with other devices authenticated as in the

Art Unit: 2135

trust group using the public/private key pair; and the security initializer further operational to receive the public/private key pair from the branding device while securely networked to the networked computing device, and further operational to initialize the security resolver with the public/private key pair" in (Col 11 lines 5-65).

Response to Arguments

21. Applicant's arguments filed on 02/27/06 have been fully considered but they are not persuasive.
22. As per argument on page 8, Applicant argues that Butt does not teach or suggest a trust group membership certificate authenticating that a device is a member of a trust group because Butt's disclosure of a session certificate comprising group membership information describes membership information for users, not devices. Examiner disagrees with the applicant. Butt's invention is to utilize a core-signed session certificate to bind any devices in a network into an authorized group membership using the information of the user in the core-signed session certificate. Such that, the core-signed session certificate is the trust group membership certificate and it can be authenticated a device is a member of the trust group based on the user information in the core-signed session certificate. (See Col 4 lines 1-30 in Butt)

23. As per remark on page 9, Applicant argues that "there is no motivation to combine Hind and Butt because Hind's teaching of creating individual certificates for each device teaches away from a certificate with group membership information as described in Butt." Applicant's basis of argument above is relying on Hind's teaching in Col 9 and Col 10 lines 18-23 (Applicant recited on page 9 of the remark). Examiner does not agree with the Applicant. In Col 10 lines 24-29,

"Yet another variation on the above embodiment (refers Col 10 lines 18-23) is to include additional data in extension fields within the signed certificate. Such additional fields could include, for example, user group associations, access control groups, etc. which then could be used in isolated pairing situations to allow autonomous access policy decisions to be made" (Emphasis added),

24. Hind clearly anticipates the utilization of the group membership information in the certificate for the device to allow autonomous access policy decisions. Such additional fields in the certificate can only be done prior transmitting the certificate to the device.
25. Applicant further argues that Hind uses the certificate only for communication between a central server and a device (Page 9 last

paragraph of the remark). Examiner respectfully believes that the Applicant has misinterpreted Hind's invention. Hind discloses a method of initializing a security-un-initialized device by transmitting a trust group membership certificate (Col 10 lines 24-29) from a branding device (the server). With the trust group membership certificate, the security-initialized device can authenticate another security-initialized device in the multi-access network for interaction (Col 10 lines 30-50).

26. As pointed out above, Applicant alleging Hind with two restrictions on the certificate is incorrect. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate Butt's teaching with Hinds to further clarify the limited teaching of Hind in Col 10 lines 24-29 to fully utilize a trust group membership certificate in a device in a network.

Art Unit: 2135

27. As per remark on page 10, Applicant argues that the rejection basis of claim 2 does not address specific language of claim 1. As the applicant recited portion of claim 1 in the remark:

electronically imprinting the security-un-initialized device with group membership and cryptographic key data by the branding device via the secured network medium . . .; and

initializing the security-un-initialized device to use the cryptographic key data to authenticate group membership of other devices . . ., and to provide the security-un-initialized device 's group membership to such other devices as authentication that the security-un-initialized device is a member of the trust web.

28. Examiner interpreted the “electronically imprinting” as to electronically store the group membership and cryptographic key data in the security-un-initialized device, and “the trust web” as a domain of the membership group. Such interpretation is obviously taught by Hinds in view of Butt as clearly pointed out above.

29. As per remark on page 11, Applicant argues that the rejection basis of claim 2 does not address specific language of claim 13. As the Applicant recited portion of claim 13 in the remark:

“...A security resolver operational when initialized with a branding public key to authenticate trust group membership certificates provided to the networked computing device from other devices via the network interface using the branding public key, and further operational to inhibit interaction via the network interface with other devices not authenticated as in the trust group,...”

30. Hind clearly teaches the certificate includes private/public key to authenticate the device into a trust group membership over a wireless communication channel interface (Col 9 lines 43-60). The branded key data is utilized to establish connection with other devices in the network (Col 10 lines 30-50).
31. Therefore, the basis rejection dated 10/20/05 is maintained.

Conclusion

32. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

Art Unit: 2135

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

33. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135


HOSUK SONG
PRIMARY EXAMINER